CLAIMS

We claim:

1. In a computational device for performing secret cryptographic calculations with secret numbers, a method of hiding secret information from outside observation comprising:

scheduling said calculations using a precomputed, fixed randomization schedule in such a way that externally observable parameters of the device cannot be associated to particular pieces, bits, symbols or values of said secret information.

2. The method of claim 1 in which scheduling said calculations comprises inserting dummy calculations according to a schedule associated with one of said secret numbers in the middle of calculations using the associated secret number.

3. The method of claim 2 in which the schedule uses a randomizing indicator in the form of a binary word having a length equal to that of the secret number and having a binary one in a select number of places that the secret number has a binary zero.

4. The method of claim 2 in which said dummy calculations affect a pattern of variation of power supply current consumed by the device so as to mask any correlation

between power supply current variation and said secret information.

5. The method of claim 1 in which in which said externally observable parameters include variation in power supply current.

6. The method of claim 1 in which said externally observable parameters include variation in timing of outputting results of said calculations.

7. The method of claim 1 in which said secret cryptographic calculations comprise exponentiating a long integer to the power of a large secret exponent.

8. The method of claim 7 in which exponentiating a long integer to the power of a large secret exponent comprises forming successive squares of said long integer reduced modulo a given modulus.

9. The method of claim 8 in which successive squares are performed in groups of a fixed length and the results temporarily stored.

10. The method of claim 9 further comprising selecting to multiplicatively accumulate certain ones of said stored results dependent on if corresponding bits of one of said

secret exponents is binary one or binary zero in such a way that the stored results which are selected cannot be determined from outside said device.

11. The method of claim 1 further comprising scheduling said calculations in such a way as to reduce computational effort.

12. The method of claim 11 in which said calculations include exponentiating a long integer to the power of a large secret exponent.

13. The method of claim 12 in which said large secret exponent is generated upon first commissioning said device into operation and is internally stored and never released outside the device.

14. The method of claim 12 in which said secret exponent is factorized into a product of sparse integers plus a remainder such that the total number of ones in a binary representation of said sparse integers and said remainder is a minimum.

15. The method of claim 13 further comprising generating in association with said secret exponent and storing in association therewith a precomputed pseudorandom schedule of dummy calculations to be inserted amidst calculations using said secret exponent.

16. The method of claim 15 in which said schedule of dummy calculations comprises dummy multiplications associated with a small fraction of the bits of said exponent which are equal to one particular binary bit polarity.

17. A tamper-proof computational device comprising:

an input/output interface;

a memory storing secret information; and

a processor operatively connected to the input/output interface and to the memory, the processor being programmed for performing secret cryptographic calculations with secret numbers and hiding said stored secret information from outside observation by scheduling said calculations using a precomputed, fixed randomization schedule in such a way that externally observable parameters cannot be associated to particular pieces, bits, symbols or values of said secret information.

18. The device of claim 17 wherein said processor schedules said calculations by inserting dummy calculations according to the precomputed, fixed randomization schedule associated with one of said secret numbers in the middle of calculations using the associated secret number.

19. The device of claim 18 in which the processor uses a randomizing indicator in the form of a binary word having a length equal to that of the secret number and having a binary one in a select number of places that the secret number has a binary zero..

20. The device of claim 18 in which said dummy calculations affect a pattern of variation of power supply current consumed by the device so as to mask any correlation between power supply current variation and said secret information.

21. The device of claim 17 in which in which said externally observable parameters include variation in power supply current.

22. The device of claim 17 in which said externally observable parameters include variation in timing of outputting results of said calculations.

23. The device of claim 17 in which said secret cryptographic calculations comprise exponentiating a long integer to the power of a large secret exponent.

24. The device of claim 23 in which exponentiating a long integer to the power of a large secret exponent comprises forming successive squares of said long integer reduced modulo a given modulus.

25. The device of claim 24 in which successive squares are performed in groups of a fixed length and the results temporarily stored.

26. The device of claim 25 wherein said processor selects to multiplicatively accumulate certain ones of said stored results dependent on if corresponding bits of one of said secret exponents is binary one or binary zero in such a way that the stored results which are selected cannot be determined from outside said device.

27. The device of claim 17 wherein said processor schedules said calculations in such a way as to reduce computational effort.

28. The device of claim 27 wherein said calculations include exponentiating a long integer to the power of a large secret exponent.

29. The device of claim 28 wherein said large secret exponent is generated upon first commissioning said device into operation and is internally stored and never released outside the device.

30. The device of claim 28 wherein said secret exponent is factorized into a product of sparse integers plus a remainder such that the total number of ones in a binary representation of said sparse integers and said remainder is a minimum.

31. The device of claim 29 wherein said processor generates in association with said secret exponent and storing in said memory in association therewith a precomputed pseudorandom schedule of dummy calculations to be inserted amidst calculations using said secret exponent.

32. The device of claim 31 wherein said schedule of dummy calculations comprises dummy multiplications associated with a small fraction of the bits of said exponent which are equal to one particular binary bit polarity.

33. The device of claim 17 wherein device comprises a smart card.

34. A mobile terminal used in a mobile communications system comprising:

a transmitter and a receiver for communicating in the mobile communications system;

a controller controlling operation of the transmitter and the receiver; and

a tamper-proof device removably, operatively connectable to the processor and comprising an input/output interface, a memory storing secret information, and a processor operatively connected to the input/output interface and to the memory, the processor being programmed for performing secret cryptographic calculations with secret numbers and hiding said stored secret information from outside observation by scheduling said calculations using a precomputed, fixed randomization schedule in such a way that externally observable parameters cannot be associated to particular pieces, bits, symbols or values of said secret information.

35. The mobile terminal of claim 34 wherein said processor schedules said calculations by inserting dummy calculations according to the precomputed, fixed randomization schedule associated with one of said secret numbers in the middle of calculations using the associated secret number.

36. The mobile terminal of claim 35 in which the processor uses a randomizing indicator in the form of a binary word having a length equal to that of the secret number and having a binary one in a select number of places that the secret number has a binary zero.

37. The mobile terminal of claim 35 in which said dummy calculations affect a pattern of variation of power supply current consumed by the device so as to mask any correlation between power supply current variation and said secret information.

38. The mobile terminal of claim 34 in which said secret cryptographic calculations comprise exponentiating a long integer to the power of a large secret exponent.

39. The mobile terminal of claim 38 in which exponentiating a long integer to the power of a large secret exponent comprises forming successive squares of said long integer reduced modulo a given modulus.

40. The mobile terminal of claim 39 in which successive squares are performed in groups of a fixed length and the results temporarily stored.

41. The mobile terminal of claim 40 wherein said processor selects to multiplicatively accumulate certain ones of said stored results dependent on if corresponding bits of one of said secret exponents is binary one or binary zero in such a way that the stored results which are selected cannot be determined from outside said device.

42. The mobile terminal of claim 34 wherein said processor schedules said calculations in such a way as to reduce computational effort.

43. The mobile terminal of claim 42 wherein said calculations include exponentiating a long integer to the power of a large secret exponent.

44. The mobile terminal of claim 43 wherein said large secret exponent is generated upon first commissioning said device into operation and is internally stored and never released outside the device.

45. The mobile terminal of claim 43 wherein said secret exponent is factorized into a product of sparse integers plus a remainder such that the total number of ones in a binary representation of said sparse integers and said remainder is a minimum.

46. The mobile terminal of claim 44 wherein said processor generates in association with said secret exponent and storing in said memory in association therewith a precomputed pseudorandom schedule of dummy calculations to be inserted amidst calculations using said secret exponent.

47. The mobile terminal of claim 46 wherein said schedule of dummy calculations comprises dummy multiplications associated with a small fraction of the bits of said exponent which are equal to one particular binary bit polarity.

48. The mobile terminal of claim 34 wherein said device comprises a smart card.

49. The mobile terminal of claim 34 wherein said device comprises a subscriber identity module.

50. The mobile terminal of claim 34 wherein said secret number comprises a private cryptographic key.